CVE-2016-5744

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2016-5744
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-07-22 15:59:01 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Siemens SIMATIC WinCC 7.0 through SP3 and 7.2 allows remote attackers to read arbitrary WinCC station files via craftec

Risk And Classification

Primary CVSS: v3.0 7.5 HIGH from nvd@nist.gov

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Problem Types: CWE-200 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
2.0	nvd@nist.gov	Primary	5		AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

AV:N/AC:L/Au:N/C:P/I:N/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Siemens	Simatic Wincc	7.0	All	All	All
Application	Siemens	Simatic Wincc	7.0	sp1	All	All
Application	Siemens	Simatic Wincc	7.0	sp2	All	All
Application	Siemens	Simatic Wincc	7.0	sp3	All	All
Application	Siemens	Simatic Wincc	7.2	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
Siemens	af854a3a-2127-4
Siemens SIMATIC WinCC Unspecified Bugs Let Remote Users Obtain Files and Execute Arbitrary Code - SecurityTracker	af854a3a-2127-4
Siemens SIMATIC WinCC, PCS 7, and WinCC Runtime Professional Vulnerabilities (Update C) | ICS-CERT	af854a3a-2127-4
SIMATIC WinCC CVE-2016-5744 Arbitrary File Read Vulnerability	af854a3a-2127-4
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**